2021年度 秋学期

卒　業　論　文

公的個人認証サービスを利用したデジタル遺品相続のオンライン化手法の提案

指導教員: 上原 哲太郎

立命館大学 情報理工学部

卒業研究3 (BA)

コース: セキュリティネットワーク

学生証番号: 2600180054-9

氏名: 太田 晃

目 次

第 1 章　研究背景 **4**

第 2 章　関連技術と問題点 **6**
2.1　デジタル遺品の問題点 6
2.2　相続 6
2.3　遺言書 7
2.4　公開鍵暗号 7
2.5　電子署名 8
2.6　電子証明書 8
2.7　公的個人認証サービス 8
2.7.1　公的個人認証サービスにおける電子証明書 9
2.7.2　公的個人認証サービスにおける電子証明書の検証 9
2.8　マイナンバーカード 10
2.9　タイムスタンプ 10
2.10 マルチシグネチャ 11

第 3 章　公的個人認証サービスを利用したデジタル遺品相続サービス **12**
3.1　相続を電子化する上での問題 12
3.2　問題解決へのアプローチ 12
3.2.1　遺言書の真正性，本人性確認 13
3.2.2　死亡確認 13
3.2.3　暗号資産の不正送金対策 13

第 4 章　提案手法 **14**
4.1　システムの設計 14
4.2　遺言書登録時の処理 15
4.3　死亡確認処理 17
4.4　相続処理 17
4.5　開発環境 18

第 5 章　結論 **19**
5.1　本研究のまとめ 19
5.2　本研究の課題 19
5.3　本研究の展望 20

参考文献 **21**

概要

様々なサービスがインターネットを通して利用することができるようになっている現在，デジタル遺品と呼ばれる個人が生前に利用していたデジタル機器に保存されたデータやインターネット上での登録情報の処理に対して，様々な問題が生じている．自身の死後のために財産処置の方法を残す手段として遺言書が存在するが，電子的な遺言書や電子的に相続を行うことのできる方法は存在していない．その理由として，遺言書のデジタル化に伴う問題や個人の認証の問題が挙げられる．一般的な遺言書は民法上で，遺言者による「自筆」が要件になっており，スキャナで電子化してもデータの特性上，第三者の検証による遺言書の真正性の証明が難しいことがある．また，相続という重要な出来事において相続人であることを証明することは非常に重要なことであり強固な認証が必要となる．そこで本論文では，電子的な相続を実行するための要件を考察し，既存の制度の活用方法と新たなシステムの導入により電子的相続を実行するための仕組みを考案する．

第1章　研究背景

近年，デジタル遺品についての問題がしばしば登場するようになった．それは，パソコンやスマホといったデジタル機器の普及に伴い，持ち主が生前に利用していた機器内に保存されているデータ，また，インターネットを通じて利用していたSNSでのやりとりや暗号資産などの各種サービスに関するデータ，すなわちデジタル遺品が増加し，遺族はそれらのデータをどのように入手しどのように対処すべきなのかという問題に直面する場面が多くなったからである．

総務省の「令和2年通信利用動向調査」[1]によると，個人のインターネット利用状況が全体で80%を越えており，年齢別にみても6歳から69歳までの各年齢層で80%を越えているなど，幅広い層でインターネットが利用されていることが分かる．また，SNSの利用状況は全体で70%を越えている．多くの個人に利用されているこれらのデジタル機器の中には様々なデータが存在しているため，デジタル遺品に関するトラブルが起きる可能性は十分に高いと考えられる．現在，個人のインターネット利用状況やSNSの利用状況では，高齢者の利用状況が約50%である．しかし，今後さらに利用割合が増加することが推測される．ここで，個人の利用者が死亡した場合，それまで故人が利用していたSNSアカウントなどインターネットサービスのアカウントが長期間放置されたままの状態になってしまう．例えば，SNSの場合はアカウントが乗っ取られて故人の名誉を傷つける恐れがあったり，悪用される可能性が高まったりする．また,「令和2年通信利用動向調査」[1]によると，SNSの利用目的として約90%が「従来からの知人とのコミュニケーションのため」と回答しているように，今やSNSはコミュニケーションのためのツールとして利用することが一般的であり，実際に会ったことはないがSNS上だけでつながっている友人がいるという人も少なくない．したがって，利用者が亡くなったことを知らせたり，生前にどのようなつながりがあったのかを調べるために遺族が故人のSNSアカウントを利用することは有用である．しかし，利用者が亡くなると，たとえ遺族であってもそのアカウントを操作して何らかの情報を得るということは困難である．実際，主要なSNSの1つである「Twitter」では，ユーザが亡くなった場合は故人との関係を証明したうえで権限のある遺産管理人または故人の家族とともにアカウントを停止，削除することはできるが，故人のアカウントのログイン情報の開示やそのアカウントを操作するといったことは，故人との関係によらず行うことができない．

また，その他のサービス，特にFX取引や有料会員サービスなどのお金に関連するサービスのアカウントが放置され，遺族に追加請求されるというリスクがある．さらに暗号資産に注目してみると放置による知らないうちに発生する被害だけでなく，相続をするときに被相続人が暗号資産を保持していたことが確認できても秘密鍵や秘密鍵を含むパスワードを知らなかった場合，実際にはその暗号資産の送金処理を行うことができないにも関わらず相続税は課税されてしまう．秘密鍵などに関して「知らない」「忘れた」ということを証明することができないからである．これらの問題を引き起こさないようにするために生前に相続人となりうる人物に周知してもらうことや死後どのようにそれらを処理すべきかといった「遺言」が重要になってくる．

自筆証書遺言書保管制度という法務局によって自筆遺言書を管理・保管してくれるサービスがはじめられた．しかし，電子的な遺言書を残し，オンライン上で相続をすることができる仕組みは存在していない．これには，電子的な遺言書が認められていないことや被相続人の死亡確認及び相続人の本人確認をオンライン上で行う仕組みが利用されていないことが関係している．

遺言書民法において本文全体，氏名及び日付を自筆し，押印しなければならなくワープロなどにより電子的に

作成された遺言書は有効としないとされている．これは筆跡や氏名をもとに遺言書作成者を特定するためである．つまり，遺言書の作成者を特定することが可能であるならば電子的な遺言書でも効力を認められてもよいのではないかと考える．そこで，本論文ではオンライン上での相続に必要な仕組み，制度を考察し，それをもとにどのようなシステムであれば電子的な相続として成立するのかということを考案する．

第2章　関連技術と問題点

2.1　デジタル遺品の問題点

通常，遺品の相続人に当たる人物が機器内に残されたデータや機器を元に，相続するためのものや連絡のための交友関係の把握のために手がかりを探し始める．しかし，機器内には多くの情報が蓄積されているため，機器が複数の相続人による共有の状態になり，ロック解除のために他の相続人の了解をとる必要があるなど手間がかかる．ただ，多くの場合において ID やパスワードと言ったログイン情報が分からず，デジタル機器そのものへのアクセスをすることができない．そこで，デジタル機器のロックを解除するためにパスワードの解析を行ってくれる業者にお願いして，機器のロックを解除しようとする．しかし，パスワードの解析が必ず成功するわけではない．仮にパスワードが判明，もしくは事前に知っていて機器のロックを解除することに成功し，その機器で故人がどのようなサービスを利用していたかを知ることができたとしても，そのサービスで利用していたアカウントへのログインのための情報までは分からない．また，どのようなやり取りが行われていたのか，どのようなデータが管理されていたかを知ることは非常に難しい．故人が利用していたサービスが判明すれば，そのサービスの運営サイトを訪れ，相続の手続きを行うことができるかもしれない．しかし，運営サイトによる相続手続きを行うためには多くの場合，正当な相続人であることを証明する必要があり，その証明ために死亡証明書や戸籍情報などの紙媒体の情報を郵送するなど手続きが煩雑化している．また，SNS を含めた多くのサービスは基本的にアカウント自体の相続を利用規約により禁止している場合が多く，正当な相続人であっても利用規約違反になることがあるなど規制が多い．

2.2　相続

相続とは，故人である被相続人の財産を特定の人物に引き継ぐことであり，被相続人が亡くなったときに発生するものである．相続は，被相続人によって書かれた遺言書があれば原則はその遺言書に沿って行われる．遺言書がない場合は民法で定められている割合に応じて相続を行う法定相続となるか，相続人全員による遺産の分割協議によって財産を分ける場合が存在する．

遺産を受け継ぐ人物は，民法で定められている順位に応じて決定される法定相続人と遺言書で指定された受遺者である．被相続人に配偶者がいる場合，配偶者は常に法定相続人となり，その他は直系卑属，直系尊属，兄弟姉妹の順で法定相続人となる可能性がある．直系卑属とは被相続人の子供またはその代襲相続人である．直系卑属とは被相続人の父母や祖父母である．第一順位の人物である直系卑属がいない場合にのみ第二順位である直系尊属が法定相続人となるといったように，順位が上の人物がいない場合は，その次の順位の人物が法定相続人となる．

相続の対象となる遺産には，現金や有価証券，車や土地，権利など有形無形の相続人にとって利益になるものだけでなく，借金や債務といった損失をともなうものもある．しかし，相続人が必ず全ての遺産を相続しなければならないわけでなく，相続を放棄することや相続人全員の同意がいるが，債務の支払いの結果利益になる範囲にとどめるような相続をすることもできる．

遺留分とよばれる，相続人が必ず相続できる最低限の遺産の割合が存在する．たとえ遺言によって財産の相続先をどのように指定されたとしても遺留分侵害額請求を行うことで遺留分を相続することができる．しかし，遺留分侵害額請求をできる人物は，兄弟姉妹でない法定相続人でありかつその相続において相続人である人物のみである．請求できる遺留分の割合は法定相続人の順位やその組み合わせによって明確に決められている．

2.3 遺言書

普通方式遺言書には，大きく分けて「自筆証書遺言」,「公正証書遺言」,「秘密証書遺言」の 3 種類があり，本稿で注目すべきものは,「自筆証書遺言」である．2020 年 7 月 10 日に法務局による遺言書の預かりサービスとして「自筆証書遺言書保管制度」が開始された [2]．しかし，この制度で預かりが可能なのは「自筆証書遺言」であり，その名の通り「自筆」であることが重要視されている．民法第 968 条 1 項により「自筆証書によって遺言をするには，遺言者が，その全文，日付及び氏名を自書し，これに印を押さなければならない.」と記されている．しかし，2019 年 1 月 13 日に施行された民法第 968 条の改正により，遺言書の財産目録についてはワープロ等の作成が認められ自筆である必要がなくなったが，依然として遺言書の本文は自筆しなければならない．自筆が重要視されている理由は，遺言は，相続をめぐるトラブルを防止するために有用な手段である．特に自筆証書遺言は自筆さえできれば遺言者本人のみで作成が可能であり，証人が不要であるなど低コストで手軽に作成することができる．しかし，遺言書の変造や偽造がなされる可能性が高く，それらが疑われたときに本当に遺言者が作成したものであるかどうかを遺言者の筆跡を元に鑑定するためである．

また，民法第 968 条第 1 項に「自筆証書によって遺言をするには，遺言者が，その全文，日付及び氏名を自書し，これに印を押さなければならない.」とある．日付の記載は，遺言書が複数発見された場合，どちらがより後に作成されたものであるかの判断を可能にし，その日付における遺言者の遺言能力の有無を判断するために利用される．遺言書に署名する氏名としては，遺言者の特定のために原則として戸籍上の本名を書かなければならないが，芸名やペンネームなどの本名以外の記載であっても「遺言者」を特定できるのであれば有効な氏名とみなしてもよいということが記されている [3]．遺言書に押す「印」については，特別な定めが存在しないため実印である必要がなく，指印でも有効性が認められる場合 [4] が存在する．しかし,「指印」による押印や押印の代わりに「花押」を書くことでは民法 968 条の要件を満たさないとして有効性が認められない場合 [5][6] も存在する．これらの有効になった事例と無効になった事例に共通している判決理由の元になっているのは，自筆による遺言書の方式に自書のほかに押印を必要としたのは，遺言の全文の自書と押印によって遺言者の同一性や真正性を確保するとともに，重要な文書は作成者による署名と押印をすることで文書の作成を完結させるということが通例であり，法に照らし合わせても文書の完成を担保するものである，という考えである．つまり，遺言者本人が正式に作成したものであることを確認することが出来るなら有効となり，確認することができないのならば無効になることが分かる．

2.4 公開鍵暗号

本稿での公開鍵暗号とは公的個人認証サービスにおいて用いられている暗号方式である RSA 暗号のことを指すものとする．公開鍵暗号では，公開鍵と秘密鍵の 2 つの鍵を 1 組のペアとして扱う．一方の鍵でメッセージの暗号化を行うと，他方の鍵でのみ復号可能である．公開鍵は他者に知られることを前提にしているのに対し，秘密鍵は絶対に他者に知られてはいないことを前提としている．公開鍵からは秘密鍵を作成できないのに対して，秘密鍵から公開鍵を作成することができ，一般に利用する際には，公開鍵で暗号文を復号するためにはそれに対応した秘密鍵を用いるためである．暗号文が第三者に入手されたとしてもその公開鍵に対応する秘密鍵を知らなければその暗号文を解読することができず，メッセージの漏洩を防ぐことができる．

2.5　電子署名

電子署名及び認証業務に関する法律 (電子署名法) では同一の法的拘束力が認められているものとして電子サインと電子署名がある．電子サインはタッチペンなどを用いて電子的にサインするものであり，手軽に利用できるものであり，対面であれば目の前にいる相手が契約書にサインする人物であるということが判断できるため有用である．しかし，対面でなければ実際に電子サインをした人物と本来の契約者が同一の人物であるということを電子サインから判別することは困難であるため，対面でないサービスでの本人確認に利用するには信頼性が低い．

電子署名は，紙文書へのサイン，押印といった真正性の証明を電子文書上で実現するための技術である．電子署名を電子文書に付与することにより，文書の改ざんやなりすましを検出することができ，その文書が原本であることが証明できる．電子署名を付与するためには，公開鍵暗号を利用する．文書の送信者は，自身の秘密鍵を用いて文書に署名を施す．受信者は，受け取った文書が本当に送信者によって署名されたものであるかを送信者の公開鍵を用いて検証する．検証に成功すればその文書は真に送信者が作成したものであり，署名付与以降に改ざんされていないことが確認できる．

2.6　電子証明書

電子署名が施された文書の署名検証を行うとき，送信者の公開鍵を用いるが，公開鍵が本当に送信者のものであるという証明が必要である．この証明のために電子証明書が必要となる．電子証明書を信頼するべきか否かを判断する規準として，電子証明書にはその電子証明書の発行者や有効期間，公開鍵の所有者の情報などが記載されており，信頼できる第三者 (認証局) によって電子署名がなされている．認証局とは，認証業務運用規定やプライバシーポリシーなどを公開し，信用できることを公に認められている機関であり，公的個人認証サービスにおいては，地方公共団体情報システム機構 (J-LIS) が認証局の役割を務めている．

2.7　公的個人認証サービス

公的個人認証サービスとは，オンラインでの申請や届け出といった行政手続きやインターネットサイトへのログインを行う際に用いられる本人確認の手段である．本人確認には，マイナンバーカードに搭載されている電子証明書を利用する．マイナンバーカードに搭載される電子証明書は地方公共団体情報システム機構 (J-LIS) により発行されており，マイナンバーカードは耐タンパー性を有しているため，マイナンバーカード内の情報が不正に読みだされたり解析されようとした場合，その内容が自動的に消去されるという対抗措置が講じられている．マイナンバーカードに搭載されている電子証明書を読み取ることで，電子署名やユーザ認証を行うことができる．公的個人認証サービスは，マイナンバー制度が開始される以前，2004 年 1 月 29 日に個人向けのサービスとして電子証明書の発行が開始されたが，これは，オンラインで行政機関への届け出などを行った人物が本当に住民基本台帳に記録されている人物であるかを確認する仕組みであり，住民基本台帳ネットワークシステムとして存在していた．このシステムでの公的個人認証サービスを利用するためには，住所地市町村に申請して住民基本台帳カードを交付してもらい，その IC チップに電子証明書と秘密鍵を格納する必要があった．以前の公的個人認証サービスによる電子証明書や電子署名の利用は，行政手続きをオンラインで行う場合にのみ利用可能であった．しかし，2013 年 5 月 31 日に公布された社会保障・税番号制度関連四法によって，公的個人認証法の一部が改正 [7] され，公的個人認証サービスの利用範囲が変更された．電子証明書の発行者が都道府県知事から J-LIS に変更され,「利用者証明用電子証明書」という電子証明書の新設がなされた．さらに，全国民に個人番号が付番されることとなり，2016 年 1 月から住民基本台帳に記録されている者に対し，その者の申請により，個人番号カードが交付され

るようになりそれに伴い，住民基本台帳カードの発行が終了するため，電子証明書格納媒体が住民基本台帳カードからマイナンバーカードに変更された．加えて，民間事業者においても電子署名や電子証明書による本人確認サービスが利用可能になった．この業務のことを特定認証業務といい，2016 年 1 月より，総務大臣による認定を受けた民間企業は総務大臣認定事業者となりマイナンバーカードの電子証明書の署名検証・利用者証明検証業務を行うことが可能になった．2022 年 1 月時点での総務大臣認定事業者は 17 社である [8].

2.7.1 公的個人認証サービスにおける電子証明書

現在の公的個人認証サービスでは，二種類の電子証明書が標準で提供されている．署名用電子証明書と利用者証明用電子証明書の 2 つである．署名用電子証明書と利用者証明用電子証明書の違いは，その利用用途と個人情報の基本となる氏名，性別，住所，生年月日の 4 つの情報である基本四情報の記載があるか否か，そして失効条件である．これらの証明書の使用用途は以下の通りである．

- 署名用電子証明書
  電子文書を行政機関に提出するための署名や捺印に相当するものとして署名用電子証明書を利用して電子申請を行う．具体的には，e-Tax の電子申請を行うために利用される．電子文書を作成・送信した者が利用者本人であり，文書が改ざんされていないことを確認するために用いられる．IC カードの紛失をしたために電子証明書の失効申請をしたり，有効期間が満了したり本人が死亡した場合に加えて，住民票の基本四情報の記載が修正された場合に失効する．基本四情報が記載されている．

- 利用者証明用電子証明書
  インターネット上のサービスを利用する際に利用しているのが本人であることを証明するための手段として用いられる．具体的には，マイナポータルへのログインやコンビニでの住民票の交付などの公的な証明書の交付サービスのために用いられる．IC カードの紛失をしたために電子証明書の失効申請をしたり，有効期間が満了したり本人が死亡した場合に失効する．基本四情報は記載されていない．

2.7.2 公的個人認証サービスにおける電子証明書の検証

電子証明書の署名検証の実施をする場面として，利用者が行政機関などに文書を提出した際に行政機関側が受け取った利用者の電子証明書の検証をする場面と行政機関から個人あてに返却された文書の電子証明書を検証する場面である．

利用者の電子証明書を検証が可能であるのは，電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（公的個人認証法）の第十七条に記載されている，行政機関，裁判所と特定認証業務を行う民間事業者のうち内閣総理大臣や総務大臣による認定を受けた民間事業者である．電子証明書の失効条件は先述の通りである．失効しているかを確認する方法は 2 つある．

- CRL(Certificate Revocation List)
  認証局から定期的に証明書のシリアル番号とその証明書の失効情報 (有効期限よりも前に何らかの理由で失効したもの) のリストである CRL が配布され，それをダウンロードしてシリアル番号を照会して検証する．1 つの証明書を検証するためにも CRL 全体をダウンロードする必要がある．

- OCSP(Online Certificate Status Protocol)
  CRL の代替として策定されたものであり，OCSP レスポンダと呼ばれるサーバを稼働させ，そこで CRL を

保管する．検証者は OCSP レスポンダに対して証明書のシリアル番号をもとに有効性の照会，署名付きの応答で有効性の検証を行う．電子証明書を個別に検証可能である．しかし，検証数が多くなると通信回数が多くなってしまう．

2.8　マイナンバーカード

マイナンバーカードとは，マイナンバーを保有する住民が申請すると無料で交付されるプラスチック製のカードであり，カード内に IC チップを搭載している．この IC チップ内に公的個人認証サービスで用いることができる電子証明書が搭載されており，公的な身分証明書としても利用できる IC カードである．マイナンバーカードの電子証明書の利用にはマイナンバーの使用はされていないため，番号法にふれることなく民間事業者を含めた様々な事業者が多様な用途に利用可能である．

マイナンバーカードの IC チップには 4 種類のカードアプリケーション (カード AP) が搭載されている．図 2.1 にマイナンバーカードの内部構成を示す．それぞれのカード AP の機能をまとめたものを表 1 に示す．

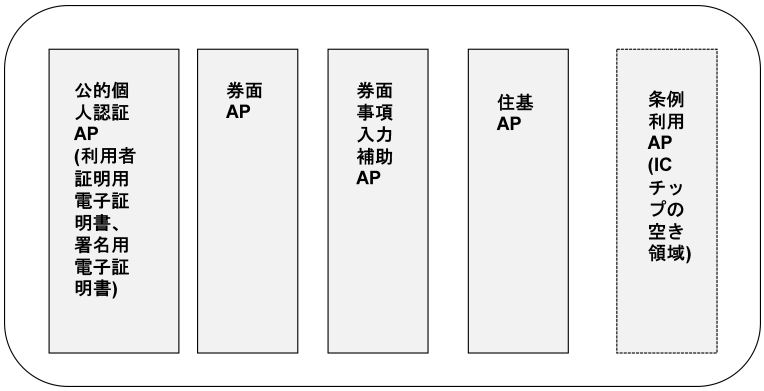

図 2.1: マイナンバーカードの AP 構成.[10] を基に作成

表 2.1: カード AP の機能.[10] を基に作成

カード AP	利用目的	暗証番号
公的個人認証 AP	署名用電子証明書:電子申請に利用 利用者証明用電子証明書:マイナポータルのログインなどに利用	6~16 桁の英数字 4 桁の数字
券面 AP	券面情報の改ざんの有無を検知	
券面事項入力補助 AP	マイナンバーや基本 4 情報をテキストデータとして利用	4 桁の数字
住基 AP	住民票コードの記録，テキストデータとして利用	4 桁の数字

2.9　タイムスタンプ

タイムスタンプとは，デジタルデータがその日時において存在していたことを証明し (存在証明)，その日時以降にデータが変更されていないことを証明する技術である．タイムスタンプを発行してもらうにはタイムスタン

プサービスの信頼の基盤でもある時刻認証局 (Time-Stamping Authority，以下「TSA」という) に特定のデータを送付する必要がある．送付するデータはメッセージダイジェストと呼ばれる，タイムスタンプを付与する元のデータのハッシュ値である．これを受け取った TSA はこのハッシュ値に時刻情報を偽造できないようにして結合したタイムスタンプトークンを送信者に送付することによりタイムスタンプを発行する．このときに付与されたタイムスタンプを検証するには TSA に送信した元のデータのハッシュ値を計算し，TSA により付与されたタイムスタンプに含まれているハッシュ値とを比較して，一致しているかを確認する．電子帳簿保存法においては電子取引の取引情報に係る電磁的記録の保存にタイムスタンプが付与されていることまたは受け取り後すぐにタイムスタンプを付すことが要件付けられているなど重要な意味を持つものである．

2.10 マルチシグネチャ

暗号資産を送金するためには，秘密鍵によりトランザクションに署名し，認証をする必要がある．その際，トランザクションの認証に複数の秘密鍵による署名を必要とする仕組みをマルチシグネチャ(以降マルチシグ) と呼ぶ．マルチシグの特徴として，単一の秘密鍵を用いて署名するシングルシグに比べて，高いセキュリティを実現できる，秘密鍵が紛失したときの対応が用意であるなどのメリットがある．しかし，全ての秘密鍵を別々の場所に保管する必要がある，複数の秘密鍵を利用するという複雑さがあるためコストがかかるといったデメリットがある．

N 個の秘密鍵のうち M 個の秘密鍵による署名により暗号資産の送金処理を可能にする場合，MofN のマルチシグと呼ぶ．2of3 マルチシグの例を図 2.2 に示す．

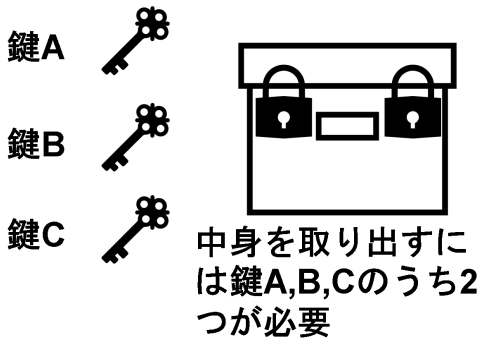

図 2.2: 2of3 マルチシグの例

第3章　公的個人認証サービスを利用したデジタル遺品相続サービス

本章では，本論文で提案する公的個人認証サービスを利用したデジタル遺品相続サービスについて述べる．

3.1　相続を電子化する上での問題

本研究では，様々なデジタル遺品の中でも特に暗号資産 (Bitcoin) と SNS(Twitter) アカウントを相続対象とする．相続を電子化する上での問題点として 4 点を取り上げる．遺言書の真正性の証明と被相続人の死亡確認，相続人の本人確認性，そして今回相続の対象としている暗号資産の送金処理を実施する際に発生する問題である．

一般的に遺言書は日付及び氏名を自筆し，押印をすることが要件とされている．しかし，要件を満たした紙の遺言書をそのままスキャナで電子化したとしても有効な遺言書とは認められない．その理由としては，遺言書の筆跡や押印により真正性の証明を行うことができなくなっているからである．つまり，電子化した遺言書を有効にするためにはその真正性を第三者によって検証，確認できることが求められる．

相続とは被相続人が亡くなった後に開始されるものであり，被相続人が生存している間は相続が発生してはいけない．電子的に死亡確認をする方法として一般的なものは存在しない．あるサービスを長期間利用していないことや SNS などによる死亡報告をもって死亡とするのは信憑性があまりにも乏しい．信頼できる機関である行政機関による報告などの信頼性のある確認が必要である．

相続人になりうる人物は基本的には親族であり，対面で相続を行う場合は相続人本人であることを確認することは容易である．しかし，電子的に行う場合，特に相続という重要な場面においての本人確認には強固な確認が必要となる．

通常，暗号資産はアドレスの管理者が保持しているアドレスに対応する秘密鍵を利用することで送金処理を完了することができる．しかし，暗号資産を相続するとなると管理者であった被相続人は死亡しているため，暗号資産の相続を行う際に被相続人が関与することはできない．暗号資産の相続を行うときに被相続人が保持していた秘密鍵を使用せずとも送金を可能にする必要がある．

3.2　問題解決へのアプローチ

3.1 で述べた問題に対し，本論文では，公的個人認証サービスを利用したデジタル遺品相続サービスを提案する．本手法は，真正性や本人確認性に対する問題に対して公的個人認証サービス，不正送金対策に暗号資産で利用されている技術を用いることで前述の問題の解決を目指す．本提案手法の要件を 3.2.1〜3.2.3 に示す．

3.2.1 遺言書の真正性，本人性確認

電子化された遺言書の問題の解決には，電子化された遺言書の真正性を証明することにより解決される．遺言書を登録する際には，登録者と遺言書保管所間で遺言書のやり取りを行う必要がある．しかし，その遺言書は本当にその登録者が作成したものであり，遺言書作成以降に誰にも改ざんがなされていないものであるという保証はない．そこで，本提案手法では電子署名に利用する公開鍵・秘密鍵のペアに公的個人認証サービスを利用する．また，タイムスタンプも付与する．公的個人認証サービスで提供されている署名用電子証明書を利用して署名を行うことにより，J-LIS によって認証されている鍵ペアを利用することができ，遺言書の真正性が保証される．さらに，タイムスタンプを検証することによりタイムスタンプの付与以降に改ざんされていないこと，遺言書作成日の証明が可能になる．また，公的個人認証サービスで提供されている利用者証明用電子証明書を利用することにより，相続人の本人性確認が J-LIS によって担保される．

3.2.2 死亡確認

相続の開始は登録者 (被相続人) の死亡が確認されたことによって開始されるべきであり，死亡の確認がなされていないにも関わらず相続が開始してしまうことは避けなければならない．また，死亡報告がされてもその真偽が確認できることが重要であり，利害関係者となる相続人による被相続人の死亡報告では信頼度が十分であるとはいえない．いまや死亡届はインターネットからダウンロードすることが可能であり，死亡届を偽造することも容易になっている．利害関係者ではない信頼できる第三者による報告が重要である．信頼できる第三者であり個人が無償で利用できる公的個人認証サービスで用いる利用者証明用電子証明書の失効情報をもとに判断する．しかし，現在の公的個人認証サービスの電子証明書の失効条件からでは，利用者の「死亡」または「海外転出」を検知することはできるが,「死亡」のみを検知することはできない．そこで，本提案手法では，公的個人認証サービスに除票となるものを導入し，より詳細な失効理由を記載可能にしそれを公開する．遺言書保管所は除票に記載された情報を確認し,「死亡」であった場合にのみ相続手続きを開始することにより，信頼性のある死亡確認を行うことができる．

3.2.3 暗号資産の不正送金対策

本提案手法では，遺言書を登録する前に被相続人とサービス実施者が連携して相続のためのアドレスを作成してもらう．送金処理に必要となる秘密鍵を被相続人のみが管理するのではなく，被相続人と相続人，サービス実施者に分散して管理することで，遺言書内にアドレスの秘密鍵を記載，遺言書を登録する際に別途秘密鍵を送信する必要がなくなる．これにより，不特定の相手に秘密鍵が漏洩することもなくなる．また，マルチシグの性質を活用することにより相続人単体だけでは送金処理を完了することができず，相続人による送金処理の完了には被相続人または遺言書保管所が管理している秘密鍵が必要になるため，相続手続き開始前に相続人による暗号資産の不正送金を防ぐことができる．

第4章　提案手法

4.1　システムの設計

相続関連業務は信託業務にあたるため，相続の執行人となる遺言書保管所は，信託業法第 3 条により内閣総理大臣の免許を受けた者でなければ営業することはできない．加えて，内閣総理大臣の免許を受けるためには，信託業法第 4 条に則った申請をする必要があるなど，法的規制も厳しい．営業の条件を満たしていたとしても遺言書保管所に相当な信頼がなければ，利用者は安心してサービスを利用することはできない．そのため，遺言書保管所には，法務省や法務局など相続関連業務を行う行政機関，もしくはすでに信託業務をしていて実績のある信託銀行により信頼性を担保されていることを証明するために官報や通知により URL などの案内をするという処置が必要である．

また，本提案手法では遺言書に記載する暗号資産のアドレスをもつ 2of4 のマルチシグウォレットは遺言書保管所と登録人が相互やり取りで作成しているものとし，その秘密鍵を遺言書保管所が 2 つ，登録人が 1 つ，そして，登録人が相続させたい相手に対して 1 つ渡しているものとする．また，相続人が 2 人以上いる場合は相続人の人数分のウォレットを作成しているものとする．

さらに，本研究で相続対象としているものである Twitter アカウントについても事前に登録してもらう必要がある．ただし，Twitter アカウントのログイン情報である ID やパスワードを登録するのではなく，Twitter API によって選択をすることができる権限を選択して登録してもらうというものである．ログイン情報を遺言書に記載してしまうと，遺言書登録以降にパスワードの変更ができなくなってしまう．遺言書を他人に盗聴された場合，認知しないうちに不正にアクセスによるなりすましがされてしまう恐れがあるなどのリスクが生じるからである．また，権限を設定しておくことで自身の死後に見られたくない情報へのアクセスを防ぐプライバシー保護の目的もある．しかし、Twitter API によって選択できるのは，読み込み，読み込みと書き込み，読み込みと書き込みとダイレクトメッセージの閲覧と送信，という 3 つの権限レベルのみである．データ単位での設定や書き込みのみを許可する権限の設定はできない．

以上を終えた後，登録者は遺言書保管所に自身の遺言書を登録してもらうための準備を行う．登録者が遺言書を保管所に登録するための事前準備の構成図を図 4.1 に示す．

IC カードと IC カードリーダ間の通信をするための規格である APDU(Application Protocol Data Unit)[11] コマンドをマイナンバーカードに送信することで電子署名を実現することができる．ただし，マイナンバーカードで行う署名は，カードへ送信したデータをカード内の秘密鍵で暗号化し返送しているだけでありカード外へ秘密鍵を取り出すことは不可能になっている．署名アルゴリズムには sha256RSA が使用されており，公開鍵は証明書の中に含まれているため証明書ファイルも取り出している．この操作を可能にするには，マイナンバーカードを取得する際に登録したパスワードが必要であるため，パスワードが漏洩していない限りは自身のマイナンバーカードを使用して他人が遺言書に署名を付すことはできなくなっている．

本手法で行っているのは署名用電子証明書の秘密鍵を用いた電子署名である．マイナンバーカードを用いた電子署名では電子申請の際に文書の作成者を証明するためには署名用電子証明書を用いることが一般的であることや 15 歳未満には実印に相当する署名用電子証明書の発行は行われないためである．加えて，民法第 961 条により

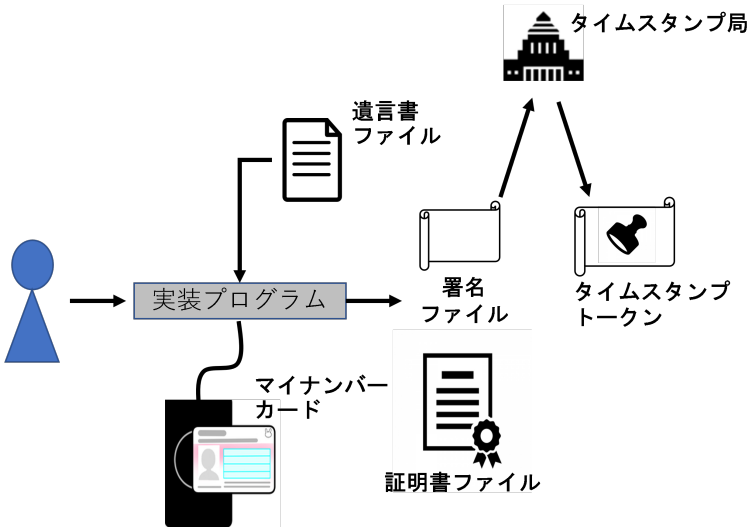

図 4.1: 事前準備処理

遺言をするための意思能力は 15 歳になってからであることも理由の一つである．

4.2 遺言書登録時の処理

遺言書には「自筆証書遺言」を利用する．理由としては，公正証書遺言や秘密証書遺言は作成のために手間や費用がかかることや作成時に立会人や法定証人の二人以上の参加が必要になるなど電子的に手続きを行うための障害になるからである．しかし,「自筆証書遺言」では内容が適切に書けていたとしても形式に不備がある場合には無効な遺言書とされてしまう．そのため，遺言書のテンプレートを配布しておき，それに遺言を記入してもらうこととする．しかしそれだけでは，登録者のミスにより遺言書の形式が崩れてしまい遺言書自体が無効になってしまう恐れがあるため，遺言書登録時に有効な遺言書の形式であるかを確認する必要がある．登録者が遺言書を保管所に登録する際の構成図を図 4.2 に示す．

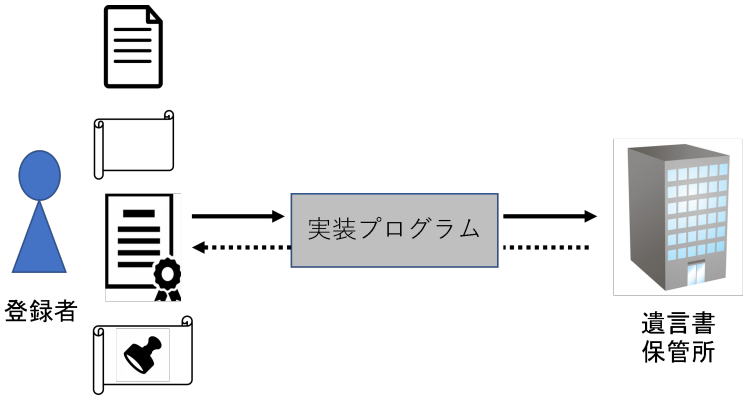

図 4.2: 遺言登録時の処理

登録者は実装プログラムに対し事前準備で作成したファイル群を実装プログラムを通して送信する．遺言書は

xml 形式で作成されており，保管所側は遺言書の登録を済ませる前に XML Schema による検証，遺言書の署名の検証，タイムスタンプの検証の 3 つによって遺言書の形式確認を行う．本システムでアップロードするファイルは，以下の 4 点である．

- **遺言書**
  登録したい遺言書ファイル本体である．
- **署名付き遺言書**
  署名用電子証明書の秘密鍵で署名された遺言書ファイルであり，遺言書の非改ざん証明に使用される．
- **署名用電子証明書**
  本人性確認と公開鍵を取り出し署名検証をするために使用される．
- **タイムスタンプトークン**
  遺言書の存在証明と非改ざん証明に使用される．

実装プログラムは，遺言保管所に遺言書を登録する前に送信された遺言書が正しいものであるかを判定する．ここでいう遺言書が正しいとは，登録者である被相続人が遺言能力を有しており，形式的に正しい遺言書であるという 2 つの要件を満たしているもののことである．遺言能力を有していることを確認するためには民法第 961 条より，満 15 歳以上である必要がある．さらに，正常な判断能力を有している必要があるがそれについての明確な定義が存在しない．そのため，遺言書の登録者が満 15 歳以上であること，形式的に正しい遺言書である，という 2 つをもって正しい遺言書であるとする．

事前準備のための実装プログラムではマイナンバーカードの署名用電子証明書による署名を行うが，マイナンバーカードを用いた署名方法には利用者証明用電子証明書を用いるものも存在する．利用者証明用電子証明書は 15 歳未満の者であっても発行されるため，電子署名を検証するだけではその署名に用いられた証明書が署名用電子証明書であるのか利用者証明用電子証明書であるのかが確認できず，登録者が満 15 歳以上であることが確認できない．そこで，まず実装プログラムは，アップロードされた電子証明書が署名用電子証明書であることを確認する．

次に，実装プログラムが行うことは，XML Schema による遺言書ファイルの検証である．XML Schema による確認により，データの正しさの検証を行い，本来想定している遺言書と全く関係のないファイルの誤登録を防ぐことができる．

その後，実装プログラムは，遺言書の署名・タイムスタンプトークンの検証を行う．遺言書の署名を受信した署名用電子証明書の公開鍵を用いて検証することで，遺言書の真正性を確認する．また，タイムスタンプトークンの検証をすることにより遺言書作成日の特定やタイムスタンプが付与された以降に改変されたいないことを二重に確認する．

最後に，遺言書登録時点で証明書が失効していると，先述した電子署名による本人証明や非改ざん証明が意味をなさなくなるため，署名用電子証明書の有効性を確認した後に登録する．一度有効性が認められ遺言書が正式に登録されたならば，電子署名に利用した証明書が有効期限切れにより失効したとしても問題はない．しかし，電子署名に利用した秘密鍵の漏洩や暗号アルゴリズムの危殆化など重大な理由によって失効した場合，登録された遺言書を破棄するなどの処置が必要になる．

遺言書が登録されると，遺言書保管所側から登録者に遺言書の「預り証」を発行する．預り証には，登録された内容物と登録者名，登録を受けた日付，預り証の発行機関名，預り証番号が記載されている．その預り証に遺

言書保管所による電子署名とタイムスタンプを付与したものを登録者に返送する．遺言書登録以降の処理に，この預り証を用いることで円滑に手続きを進めることができる．

4.3 死亡確認処理

遺言書保管所による被相続人の死亡確認の処理は，マイナンバーカードの利用者証明用電子証明書の失効および，その失効理由を新たに導入する JPKI の除票での検証により確認を可能にする．この除票は地方公共団体システム機構により 24 時間ごとに発行される．ただし，除票にアクセスもしくはダウンロードが可能なのは現行の JPKI の CRL と同様に署名検証者または団体署名検証者のみとする．図 4.3 に死亡確認処理の構成図を示す．

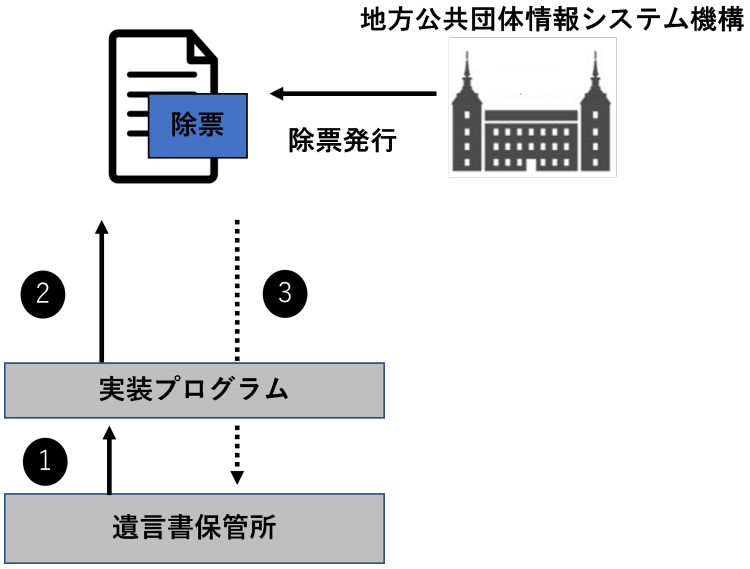

図 4.3: 死亡確認処理

死亡確認処理の動作手順は，次の通りである．
① 遺言書保管所は登録者の利用者証明用電子証明書の失効確認を実装プログラムに要求する．
② 実装プログラムは地方公共団体システム機構により発行された除票にアクセス，ダウンロードをする．
③ 実装プログラムは利用者証明用電子証明書の失効確認の結果，失効しているならその理由を遺言書保管所に通知する．

4.4 相続処理

相続処理は遺言保管所による死亡確認処理が完了した後にのみ実行される処理である．例え相続人からの申請があったとしても被相続人の死亡確認処理が完了していない場合には処理されない．

相続を行う相手は遺言書に記載されている相続人である必要があるため，相続処理を行う際には相続人の認証を行う．相続人の認証には，マイナンバーカードの利用者証明用電子証明書による本人認証を用いる．これは，コンビニエンスストアでの住民票交付など証明書の交付が受けられるサービスでも利用されている方法でもある．こ

れを用いることにより，公的個人認証サービスによる信頼性のある認証をすることができるほか，その際に取得したマイナンバーを利用することで相続の申請を行った相続人を識別することができるようになる．しかし，そのような機能を完備したプログラムの作成は実装することができなかったため，マイナンバーカードからマイナンバーを取りだし，相続人の識別のみを行うプログラムとなっている．

相続人の認証が完了したのち，遺言書に記載されている相続人毎の遺言の内容に応じた手続きする．本研究で実装した相続対象となる内容は，Bitcoin と Twitter アカウントの操作権限である．

Bitcoin の相続は，遺言書に記載されているアドレスに対応した，遺言書保管所が所持している秘密鍵と相続人が所持している秘密鍵を用いて処理を行う．そのため，公的個人認証サービスを利用した相続人認証と相続対象アドレスに対応した秘密鍵を保持していることによる認証の 2 つを利用することとなり，強固な認証を行ったうえで送金処理を可能にする．

4.5　開発環境

本システムは表 4.1 に示す開発環境で開発された．相続に利用するマルチシグウォレットおよびアドレスの作成は python のライブラリである bitcoinlib[12] を利用した．相続する Twitter アカウントの権限設定のための Twitter API を操作するために php のライブラリである twitteroauth[13] を使用した．マイナンバーカードとの通信には，Python ライブラリの pyscard[14] で提供されている機能を使用した．署名・証明書の検証などの暗号化関数の利用には，OpenSSL[15] を用いた．

表 4.1: 開発環境.

ハードウェア・ソフトウェア	環境	バージョン
カードリーダー	SMART ATM CARD READER	-
暗号資産ライブラリ	bitcoinlib	0.6.3
Twitter API ライブラリ	twitteroauth	3.1.0
スマートカードライブラリ	pyscard	2.0.2
暗号ライブラリ	OpenSSL	1.1.1k

第5章　結論

5.1　本研究のまとめ

本研究では，デジタル遺品の処理にともなうトラブルに着目し，その問題として相続の電子化を設定した．問題解決のアプローチとして，遺言書の電子化とそれに付随した相続のオンライン化の提案とその手法について提案した．

提案手法では，遺言書の電子化へのアプローチとして，元来自筆が要件とされている自筆証書遺言をもとに，XML Schema による遺言書の形式確認，遺言書の真正性の担保をするために，遺言書をマイナンバーカードに搭載される署名用電子証明書の秘密鍵で署名し，署名時に利用した証明書とともに登録した．また，遺言書にタイムスタンプを付与，検証可能な状態で公開することにより，遺言書作成日の特定と作成日時以降の非改ざん証明をすることに成功した．

また，提案手法では，公的個人認証サービスに除票を導入し，細分化した証明書の失効理由をもとに死亡確認を実施することにより，オンライン上でも厳格で信頼性のある死亡確認を実現することを可能にした．

本提案手法を用いることで，限定的ではあるが相続人の本人確認性がともなったデジタル遺品のオンライン相続の実行を可能にした．

5.2　本研究の課題

本研究の提案手法では，被相続人や相続人の識別のためにマイナンバーを利用した．しかし実際には，被相続人や相続人の認証は JPKI によるものでありマイナンバーは識別のための情報に過ぎない．マイナンバーは「マイナンバー法」により定められた社会保障，税，災害対策の手続き以外で利用することができない．そのため，マイナンバーなどの法的な制約を受けることなく相続人の識別情報として個人を識別することが可能である情報を利用することが必要である．

相続人 1 人 1 人に対して 2of4 のウォレットを作成しているため，相続人の数が多ければその分遺言書保管所によるウォレットの管理コストが大きくなるという問題がある．また，2of4 のマルチシグウォレットのうち 2 つの秘密鍵は遺言書保管所により管理されているため遺言書保管所と相続人との共謀もしくは，遺言書保管所単体で不正に暗号資産を送金できてしまう．しかし，遺言書保管所が過半数の鍵を所持しておかなければ相続人が鍵を紛失してしまったしたときに暗号資産があるにもかかわらず送金処理ができなくなってしまう．マルチシグの特性を上手く利用し必要鍵数や鍵の管理人を増やす，鍵の分配方法を調整することで，不正送金を防ぎながら 1 人当たりの鍵管理コストを削減する方法を検討する必要がある．

被相続人の死亡後に開始された相続において，相続が完了する前に相続人 (A とする) が亡くなってしまった場合，遺留分を含めた相続可能な割合は変化しないため，A 以外の相続人には問題なく相続が可能である．しかし，通常であれば A の相続人に遺産が渡るべきである (数次相続の発生) が，本提案手法では，A が遺言書を登録していない場合，本来 A の相続人に相続されるべき遺産の送金処理自体は可能であるが A の相続人を知ること，また

その証明ができないために送金できないという問題が発生する可能性があるため，これに対応する方法について検討する必要がある．

5.3　本研究の展望

本研究では限定したデジタル遺品相続にのみ注目したものであるが，実際に相続を行う際はデジタル遺品のみでなく普通の遺産の相続が伴うことがふつうである．本研究で示した遺言書の電子化とそれに付随したサービスを用いることでデジタル遺品のみならず，普通の相続も電子的に完結させることが可能になる．

マイナンバー単体では悪用することはできないにもかかわらず，たとえ本人の許可があろうともマイナンバーを公開することは認められていない．また，マイナンバーは隠すものであるという印象はマイナンバーの活用を妨げていると推測できるためマイナンバーの秘匿を不要にする，もしくは，本人の許可があればマイナンバーの使用を認めるというようにすれば様々な場面で活用可能になると考える．マイナンバーカードやその電子証明書の仕様が一般に公開されていない．そのため，これらを活用したサービスを展開することは困難である．これらを公開することで様々なサービスや制度の基盤となる．

謝辞

本研究を行うにあたり，研究の着想から，論文執筆まで多くの助言，ご指導をしてくださいました上原哲太郎教授に心より感謝申し上げます．また，サイバーセキュリティ研究室の皆様をはじめ，本研究を行う上で支えてくださったすべての方々に感謝申し上げます．

参考文献

[1] 総務省. 令和 2 年通信利用動向調査. https://www.soumu.go.jp/johotsusintokei/statistics/data/210618_1.pdf. 閲覧日:2021-12-19.

[2] 自筆証書遺言書保管制度のご案内. https://houmukyoku.moj.go.jp/mito/page000001_00041.pdf. 閲覧日:2021-11-25.

[3] 中川善之助, 泉久雄. 相続法第 4 版.pp.514-527. 有斐閣社,2000.

[4] 遺言無効確認請求事件. https://www.courts.go.jp/app/files/hanrei_jp/210/052210_hanrei.pdf. 閲覧日:2021-12-30.

[5] 遺言書真否確認請求事件. https://www.courts.go.jp/app/files/hanrei_jp/310/020310_hanrei.pdf. 閲覧日:2021-12-30.

[6] 遺言書真正確認等，求償金等請求事件. https://www.courts.go.jp/app/files/hanrei_jp/930/085930_hanrei.pdf. 閲覧日:2021-12-30.

[7] 総務省. 公的個人認証サービス利用のための民間事業向けガイドライン. https://www.soumu.go.jp/main_content/000400619.pdf. 閲覧日:2021-10-2.

[8] 総務省. 主務大臣認定事業者. https://www.soumu.go.jp/main_content/000747198.pdf. 閲覧日:2022-1-15.

[9] 地方公共団体情報システム機構. 公的個人認証サービスポータルサイト. https://www.jpki.go.jp/procedure/period.html. 閲覧日:2021-10-2.

[10] マイナンバー制度とマイナンバーカード. https://www.soumu.go.jp/kojinbango_card/03.html. 閲覧日:2021-10-21.

[11] 密着型 IC カードの実装規約 第 4 章. https://www.nmda.or.jp/nmda/ic-card/iso10536/sec4.html.

[12] bitcoinlib. https://github.com/abraham/twitteroauth

[13] TwitterOAuth. https://github.com/1200wd/bitcoinlib

[14] pyscard. https://github.com/LudovicRousseau/pyscard

[15] OpenSSL. https://github.com/LudovicRousseau/pyscard

[16] 公的個人認証サービス (電子証明書) 中央区ホームページ. https://www.city.chuo.lg.jp/smph/kurasi/toroku/koutekikozinnninnsyuou.html. 閲覧日:2021-1-15.